Ruckus Wireless Security Advisory ID 031813-1 FAQ:

Unauthenticated TCP tunneling on Ruckus devices via SSH server process

Customer release date: ***March 25, 2013***
Public release date: ***May 27, 2013***

What is the issue?

Ruckus Wireless allows for SSH connectivity to its devices for debuggability and maintenance reasons. It was discovered that a malicious user could abuse the TCP tunneling feature of the SSH daemon on Ruckus devices to proxy random TCP streams through these devices. The user does not have to be authenticated to the Ruckus device for requesting and establishing such a tunnel. Once tunnel is established, the user's TCP stream would be carried over SSH to the Ruckus device, which would forward the traffic to an IP and port of the user's choosing.

What are the Pre-requisites for this attack?

The only pre-requisite is network access to SSH port (TCP/22) on the Ruckus device. SSH daemon is enabled by default on Ruckus devices.

How do I check if I am vulnerable?

This issue affects the following software branches and devices. Any products not mentioned in this table are **not** affected.

Ruckus Device	Affected software branch
ZoneDirector Controllers	9.2.x, 9.3.x, 9.4.x, 9.5.x
ZoneFlex Access Points	9.2.x, 9.3.x, 9.4.x, 9.5.x, 1.x.x
SmartCell Access Points	1.x.x
Smart Cell Gateway	NOT AFFECTED

Is there a way to mitigate the vulnerability?

Ruckus Wireless recommends that all customers apply the appropriate patch(es) as soon as practical. However, in the event that a patch cannot immediately be applied, the following steps will help to mitigate the risk:

- Do not expose management interfaces of Ruckus Wireless devices (including SSH access) to untrusted networks such as the Internet.
- Use a firewall to limit SSH traffic to/from Ruckus Wireless devices to trusted hosts.
- If limiting SSH access is not possible, an extreme workaround is to disable SSH access to the Ruckus device via a firewall in the path or via the HTTPS Web Interface of the device itself.

How does Ruckus Wireless qualify severity of security issues?

Ruckus Wireless utilizes the Common Vulnerability Scoring System (CVSS) v2. This rating system is a vendor agnostic, industry open standard designed to convey vulnerability severity and help determine urgency and priority of response.

CVSS v2 BASE METRIC SCORE: 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

When will this Ruckus Wireless Security Advisory be publicly posted?

In order to protect our customers and partners, we allow time for customers to upgrade systems or implement workarounds to minimize the vulnerability risk. The security advisory will be posted on publicly on **May 27, 2013.** This Ruckus Security Advisory constitutes Ruckus Proprietary Information and should not be disseminated, forwarded or disclosed without written permission from Ruckus Wireless.

Where do I download the fixed software patches?

Ruckus customers can obtain the fixed firmware from the support website at
https://support.ruckuswireless.com/

The following patches have the fix (any later patches will also have the fix):

Affected software branch	Software Patch	Recommended For
9.2.x	ZF7731_9.2.0.0.168	ZoneFlex 7731 Only
9.3.x	9.3.4.0.17	ZoneDirector 1000
9.4.x	9.4.3.0.16	ZoneDirector 1100/3000/5000
9.5.x	9.5.1.0.50	Standalone Access Points ZoneDirector 1100/3000/5000
1.x.x	1.1.1	Smart Cell Gateway

Ruckus Support can be contacted as follows:

1-855-RUCKUS1 (1-855-782-5871) (United States)
e-mail: support@ruckuswireless.com

The full contact list is at:
https://support.ruckuswireless.com/contact-us
